أمن المعلومات

GS224-10

نظام جدار الحماية (Firewall)

- يمكن أن تكون جدران الحماية وسيلة فعالة لحماية نظام محلي أو شبكة من الأنظمة من التهديدات الأمنية للشبكات وتتيح في نفس الوقت الوصول إلى العالم الخارجي عبر شبكات المترامية / الموسعة والإنترنت.
- لم يعد الاتصال بالإنترنت اختياريًا للمؤسسات ، فالمعلومات والخدمات المتاحة على الانترنت ضرورية للمنظمة. علاوة على ذلك ، يحتاج المستخدمون الأفراد داخل المؤسسة للوصول إلى الإنترنت ، وإذا لم يتم توفير ذلك عبر شبكة المحلية الخاصة بهم ، فسيستخدمون إمكانية الاتصال الهاتفي من أجهزة الحاسوب الخاصة بهم إلى مزود خدمة الإنترنت (ISP) . ويوفر الوصول إلى الإنترنت فوائد للمؤسسة ، فإنه يمكّن العالم الخارجي من الوصول إلى أصول الشبكة المحلية والتفاعل معها ، وهذا يخلق تهديدا للمنظمة.
- في حين أنه من الممكن تجهيز كل محطة عمل وخادم فى محيط الشبكة بميزات أمان قوية ، مثل الحماية من التسلل ، فإن هذا ليس نهجًا عمليًا.
- البديل ، والمقبول بشكل متزايد هو جدار الحماية الذي يتم وضعه بين محيط شبكة والإنترنت لإنشاء ارتباط متحكم به وإقامة جدار أمن على محيط الشبكة. الهدف من هذا المحيط هو حماية محيط الشبكة من الهجمات المعتمدة إلى الإنترنت وتوفير عنق مرور واحد حيث يمكن فرض الأمن والتدقيق.

سياسة الوصول لجدار الحماية

- يعد تحديد سياسة وصول مناسبة أحد المكونات الحاسمة في تخطيط جدار الحماية وتنفيذه.
  - تسرد أنواع حركة المرور المصرح لها بالمرور عبر جدار الحماية ، بما في ذلك نطاقات العناوين والبروتوكولات والتطبيقات وأنواع المحتوى.
- يجب تطوير هذه السياسة عبر تقييم المخاطر و سياسة أمن المعلومات في المنظمة.
- يجب تطوير هذه السياسة من خلال المواصفات الموسعة لأنواع حركة المرور التي تحتاج المنظمة إلى دعمها.
  - من ثم يتم تنقيحها لتحديد تفصيل عناصر التصفية ، والتي يمكن بعد ذلك تنفيذها ضمن هيكل جدار حماية مناسب.

قدرات وقيود جدار الحماية

تقع الإمكانات التالية ضمن نطاق جدار الحماية:

- يحدد جدار الحماية نقطة الاختناق التي تُبقي المستخدمين غير المصرح لهم خارج الشبكة المحمية ، ويمنع الخدمات التي يُحتمل أن تكون معرضة للخطر من دخول الشبكة أو مغادرتها ، ويوفر الحماية من أنواع مختلفة من انتحال بروتوكول الإنترنت (IP) وهجمات التوجيه. يؤدي استخدام نقطة اختناق واحدة إلى تبسيط إدارة الأمن.
- يوفر جدار الحماية موقعًا لمراقبة الأحداث المتعلقة بالأمن.
- يعد جدار الحماية نظامًا أساسيًا مناسبًا للعديد من وظائف الإنترنت الغير مؤمنة. يتضمن ذلك برتوكول مترجم عنوان الشبكة (NAT) ، ووظيفة إدارة الشبكة التي تقوم بتدقيق استخدام الإنترنت أو سجلاته.
- يمكن لجدار الحماية أن يعمل كمنصة لبرتوكول (IPSec) لانجاز الشبكات الافتراضية الخاصة.

للجدران النارية حدودها ، بما في ذلك ما يلي:

- لا يمكن لجدار الحماية الحماية من الهجمات التي تتجاوز جدار الحماية ، على سبيل المثال من الاتصال الهاتفي ، أو إمكانية الاتصال بمجمع المودم للموظفين المتنقلين والعاملين عن بُعد.
- قد لا يوفر جدار الحماية الحماية الكاملة من التهديدات الداخلية ، مثل موظف ساخط أو موظف يتعاون عن غير قصد مع مهاجم خارجي.
- قد يتم الوصول إلى شبكة محلية لاسلكية مؤمنة بشكل غير صحيح من خارج المؤسسة
- يمكن استخدام الحاسوب المحمول أو المساعد الرقمي الشخصي أو جهاز التخزين المحمول وإصابته من خارج شبكة الشركة ثم توصيله واستخدامه داخليًا.

قدرات وقيود جدار الحماية

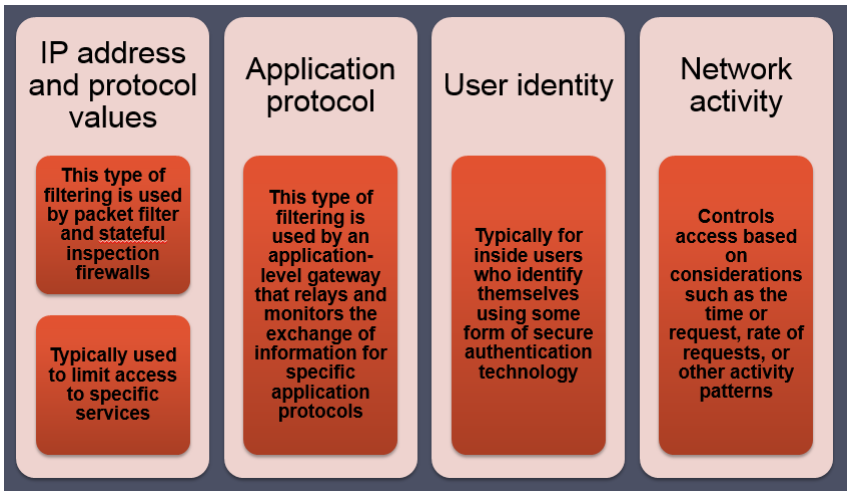
القدرات :-

- يحدد نقطة مرور واحدة
- يوفر موقعًا لمراقبة الأحداث الأمنية
- منصة مناسبة لبعض وظائف الإنترنت مثل (NAT) ، ومراقبة الاستخدام ، و IPSEC، و VPNs

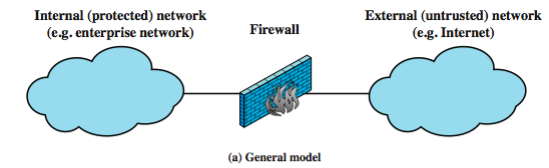
الحدود :-

- لا يمكن الحماية من الهجمات التي تتجاوز جدار الحماية
- قد لا توفر الحماية الكاملة من التهديدات الداخلية
- شبكة محلية لاسلكية آمنة بشكل غير صحيح
- الكمبيوتر المحمول ، المساعد الرقمي الشخصي ، جهاز تخزين محمول مصاب بالخارج ثم يستخدم في الداخل

خصائص مصفى جدار الحماية



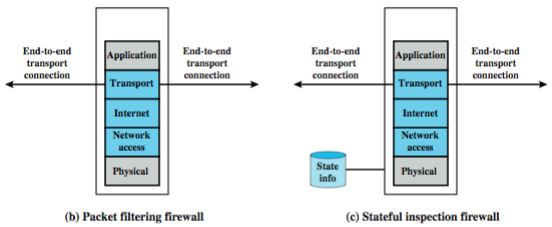
أنواع جدران الحماية



(a) General model

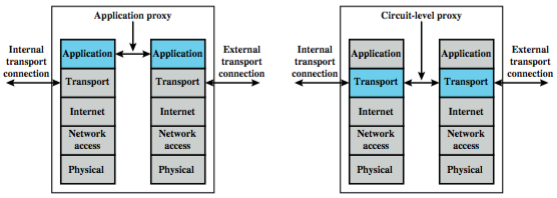
مصفى إيجابي (سلبي):
السماح (الرفض) للحزم التي تستوفي بالمعايير

فحص الحالة:
يتتبع اتصالات TCP



(b) Packet filtering firewall

(c) Stateful inspection firewall



(d) Application proxy firewall

(e) Circuit-level proxy firewall

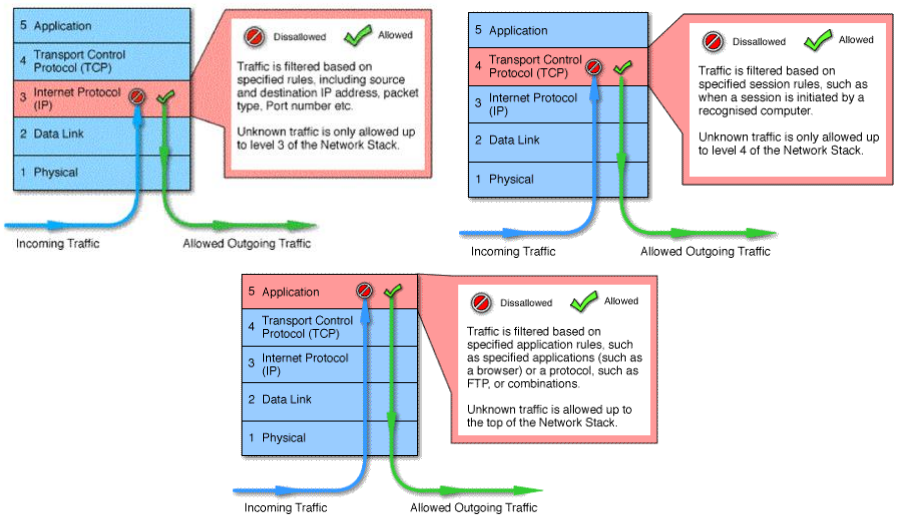
أنواع جدران الحماية

قد يعمل جدار الحماية كعامل تصفية للحزم. يمكن أن يعمل كمرشح إيجابي ، مما يسمح بتمرير الحزم التي تفي بمعايير محددة فقط ، أو كمرشح سلبي ، يرفض أي حزمة تفي بمعايير معينة. اعتمادًا على نوع جدار الحماية ، قد يفحص مقدمة بروتوكول واحد أو أكثر في كل حزمة ، أو حمولة كل حزمة ، أو النمط الذي تم إنشاؤه بواسطة سلسلة من الحزم. في هذا القسم ، نلقي نظرة على الأنواع الرئيسية لجدران الحماية ، والتي تشمل:

- **جدار حماية تصفية الحزم**: يطبق مجموعة من القواعد على كل حزمة (IP) واردة وصادرة ثم يعيد توجيه الحزمة أو يتجاهلها (الشكل ب).
- **جدران حماية تفتيش الحالة**: تستعرض نفس معلومات الحزمة مثل جدار حماية تصفية الحزمة ، ولكنها تسجل أيضًا معلومات حول اتصالات (TCP) (الشكل ج). قد يتتبع أيضًا أرقام تسلسل (TCP) لمنع الهجمات التي تعتمد بطريقة ما على الرقم التسلسلي ، مثل اختطاف الجلسة.
- **بوابة بمستوى التطبيق**: تعمل كمرحل للحركة على مستوى التطبيق (الشكل د). يتصل المستخدم بالبوابة باسم المضيف البعيد الذي سيتم الوصول إليه. عندما يستجيب المستخدم ويقدم معرف مستخدم صالح ومعلومات مصادقة ، تتصل البوابة بالتطبيق الموجود على المضيف البعيد وتنقل مقاطع (TCP) التي تحتوي على بيانات التطبيق بين النهايتين.
- **بوابة بمستوى الدائرة**: أو وكيل بمستوى الدائرة (الشكل هـ) يحدد التوصيلات التي سيتم السماح بها ، وإذا كان الأمر كذلك ، يُنشئ اتصالين (TCP)، أحدهما بينها وبين مستخدم (TCP) على مضيف داخلي والآخر بينها وبين مستخدم (TCP) على مضيف خارجي. بمجرد إنشاء التوصلين ، تقوم البوابة عادةً بترحيل مقاطع (TCP) من اتصال إلى آخر دون فحص المحتويات.

تصفية الحزم مقابل البوابة مقابل جدار الحماية بمستوى التطبيق

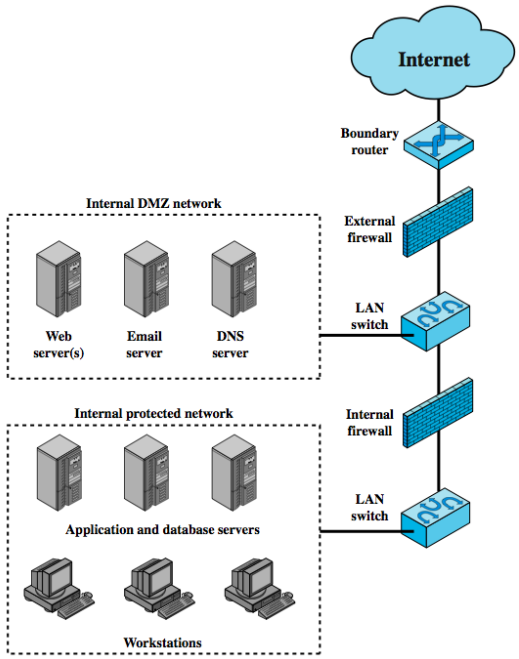
Packet Filtering vs Gateway vs Application-Level Firewall



جدار الحماية الشخصي

- يتحكم جدار الحماية الشخصي في حركة المرور بين حاسوب شخصي أو محطة عمل من جهة ، وشبكة الإنترنت أو شبكة المؤسسة على الجانب الآخر. يمكن استخدام وظيفة جدار الحماية الشخصي في بيئة المنزل وعلى إنترانت الشركة. عادةً ما يكون جدار الحماية الشخصي عبارة عن وحدة برمجية على الحاسوب الشخصي. في بيئة منزلية مع حواسيب متعددة متصلة بالإنترنت ، يمكن أيضًا وضع وظيفة جدار الحماية في جهاز توجيه يصل جميع ألحواسيب المنزلية بـجهاز (DSL) أو مودم كابل أو واجهة إنترنت أخرى. عادةً ما تكون جدران الحماية الشخصية أقل تعقيدًا بكثير من جدران الحماية المعتمدة على الخادم أو جدران الحماية المستقلة. يتمثل الدور الأساسي لجدار الحماية الشخصي في رفض الوصول غير المصرح به عن بُعد إلى الحاسوب. يمكن لجدار الحماية أيضًا مراقبة النشاط الصادر في محاولة لاكتشاف الفيروسات المتنقلة والبرامج الضارة الأخرى وحظرها.
- مثال على جدار الحماية الشخصي هو القدرة المضمنة في نظام التشغيل (Mac OS X). عندما يقوم المستخدم بتمكين جدار الحماية الشخصي في نظام التشغيل (Mac OS X)، يتم رفض جميع الاتصالات الواردة باستثناء تلك التي يسمح بها المستخدم صراحةً. لمزيد من الحماية ، قد تتوفر ميزات جدار الحماية المتقدمة ، مثل: وضع التخفي يخفي جهاز (Mac) على الإنترنت عن طريق إسقاط حزم الاتصال غير المرغوب فيها ، مما يجعله يبدو كما لو أنه لا يوجد جهاز (Mac). يمكن حظر حزم (UDP) ، مما يؤدي إلى تقييد حركة مرور الشبكة لحزم (TCP) على المنافذ المفتوحة فقط. قد يدعم جدار الحماية أيضًا تسجيل الاحداث ، وهو أداة مهمة للتحقق من النشاط غير المرغوب فيه.

مواقع جدار الحماية



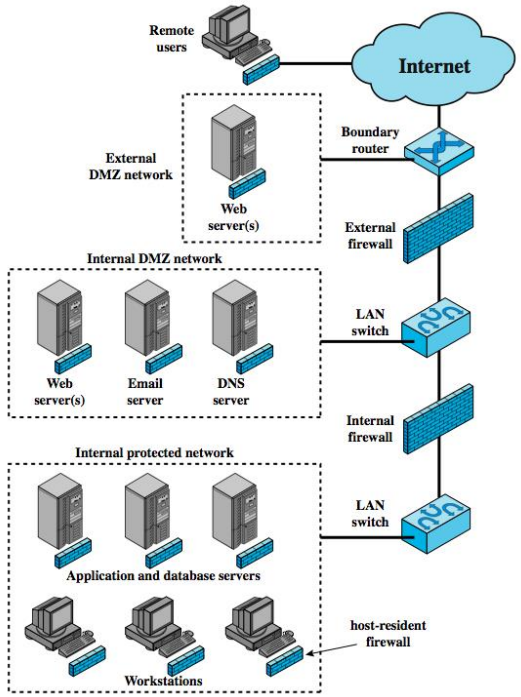
جدار الحماية الخارجي:
حماية للمنطقة منزوعة السلاح (DMZ) بما يتفق مع حاجتها للاتصال الخارجي

جدار الحماية الداخلي:
(أ) قدرة تصفية أكثر صرامة لتوفير الحماية من الهجمات الخارجية
(ب) يوفر حماية ثنائية الاتجاه لشبكة DMZ

مواقع جدار الحماية

يتم وضع جدار الحماية لتوفير حاجز وقائي بين مصدر خارجي ، يحتمل أن يكون غير موثوق به لحركة المرور والشبكة الداخلية. مع وضع هذا المبدأ العام في الاعتبار ، يجب على مسؤول الأمان تحديد الموقع وعدد جدران الحماية المطلوبة.

- يقترح الشكل التمييز الأكثر شيوعًا ، وهو التمييز بين جدار الحماية الداخلي والخارجي. يتم وضع جدار حماية خارجي على حافة شبكة محلية أو شبكة مؤسسة. يعمل جدار حماية داخلي واحد أو أكثر على حماية الجزء الأكبر من شبكة المؤسسة. بين هذين النوعين من جدران الحماية يوجد جهاز واحد أو أكثر متصل بالشبكة في منطقة يشار إليها باسم شبكة (DMZ) - المنطقة المنزوعة السلاح. عادةً ما توجد شبكات الأنظمة التي يمكنها التواصل خارجيًا ولكنها تحتاج إلى الحماية في منطقة (DMZ).
- يوفر جدار الحماية الخارجي مقياسًا للتحكم في الوصول والحماية لأنظمة (DMZ) بما يتوافق مع حاجتها للاتصال الخارجي. يوفر جدار الحماية الخارجي أيضًا مستوى أساسيًا من الحماية لبقية شبكة المؤسسة.
- في هذا النوع من التكوين ، خادم جدران الحماية الداخلية ثلاثة أغراض:
  - يضيف قدرة تصفية أكثر صرامة ، مقارنة بجدار الحماية الخارجي ، من أجل حماية خوادم المؤسسة ومحطات العمل من الهجمات الخارجية.
  - يوفر حماية ثنائية الاتجاه فيما يتعلق بالمنطقة المجردة من السلاح ، ويحمي ما تبقى من الشبكة من الهجمات التي يتم إطلاقها من المنطقة المجردة من السلاح ويحمي أنظمة DMZ من الهجوم من الشبكة الداخلية المحمية.
  - يمكن استخدام العديد من جدران الحماية الداخلية لحماية أجزاء من الشبكة الداخلية من بعضها البعض. يوضح الشكل 5 التكوين الذي يتم فيه حماية الخوادم الداخلية من محطات العمل الداخلية والعكس صحيح.



جدران الحماية الموزعة

مزيج من جدران الحماية السابقة

جدار الحماية المقيم المضيف على 100 من أجهزة الحواسيب بالإضافة إلى جدران الحماية المستقلة تحت إدارة مركزية

جدران الحماية الموزعة

- يتضمن تكوين جدار الحماية الموزع أجهزة جدار حماية مستقلة بالإضافة إلى جدران الحماية المستندة إلى المضيف والتي تعمل معًا تحت تحكم إداري مركزي. يوضح الشكل تكوين جدار حماية موزع. يمكن للمسؤولين تكوين جدران الحماية الخاصة بالمضيف على مئات الخوادم ومحطات العمل بالإضافة إلى تكوين جدران الحماية الشخصية على أنظمة المستخدم المحلية والبعيدة. تتيح الأدوات لمسؤول الشبكة تعيين السياسات ومراقبة الأمان عبر الشبكة بالكامل. تعمل جدران الحماية هذه على الحماية من الهجمات الداخلية وتوفر الحماية المصممة لأجهزة وتطبيقات معينة. توفر جدران الحماية المستقلة حماية عالمية ، بما في ذلك جدران الحماية الداخلية وجدار الحماية الخارجي ، كما تمت مناقشته سابقًا.
- مع جدران الحماية الموزعة ، قد يكون من المنطقي إنشاء منطقتي (DMZ) داخلية وخارجية. يمكن وضع خوادم الويب التي تحتاج إلى حماية أقل نظرًا لوجود معلومات أقل أهمية عليها في منطقة (DMZ) الخارجية ، بعد جدار الحماية الخارجي. الحماية المطلوبة يتم توفيرها بواسطة جدران الحماية المعتمدة إلى المضيف في هذه الخوادم.
- من الجوانب المهمة لتكوين جدار الحماية الموزع مراقبة الأمان. تتضمن هذه المراقبة عادةً تجميع السجلات وتحليلها وإحصاءات جدار الحماية والمراقبة الدقيقة عن بُعد للمضيفين الفرديين إذا لزم الأمر.